

REMARKS/ARGUMENTS

Claims 5-11 and 15-27 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 102, Asserted Anticipation

The examiner rejected claims 5-11, 15, and 18-27 under 35 U.S.C. § 102 as anticipated by *Ricciulli, Method of Maintaining Lists of Network Characteristics*, U.S. Patent 6,973,040 (December 6, 2005). This rejection is respectfully traversed.

The examiner states that:

Ricciulli discloses a computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

Obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system (Column 3, lines 16-33);

Obtaining network information, from network equipment connected to the device, regarding the attack (Column 4, line 45 to Column 5, line 2);

Determining a logical entry point (IP addresses, as well as TCP/UDP ports are logical representation used in combination to identify the entry point) of the attack using a correlation engine to correlate the intrusion information and the network information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and

Identifying a physical entry point (the physical entry point is where the router or node actually connects to the network, on its network interface) associated with the logical entry point (Column 3, lines 34-43).

Office Action of January 11, 2006, p.3.

Claim 5 is as follows:

5. (Previously Presented) A computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system;

obtaining network information, from network equipment connected to the device, regarding the attack;

determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information; and

identifying a physical entry point associated with the logical entry point.

Ricciulli does not anticipate claim 5 because *Ricciulli* does not teach the claimed step of determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information. Additionally, *Ricciulli* does not anticipate claim 5 because *Ricciulli* does not teach the claimed step of identifying a physical entry point associated with the logical entry point. The examiner's assertions to the contrary are manifestly incorrect.

Regarding the step of determining a logical entry point, the examiner asserts that two portions of *Ricciulli* teach this step. In the first portion cited by the examiner, *Ricciulli* states:

Various embodiments have routers with one or more lists of top-N more seen or most seen network characteristics, for example, destination addresses, in a small cache. This list can vary with time relatively slowly, for example, on the order of seconds for some embodiments. In some embodiments, the cache can have a number of instances of network characteristics substantially equal to or greater than C/F, where C can be a total aggregate capacity of a router, and F can be a minimum sustained flooding rate to detect. For example, to detect a 1 MB/s flooding on a 1 GB/s router, a cache of 1000 instances may be adequate. In one embodiment, listed instances can include a destination address and an ingress port.

When an attack, such as flooding, is detected, a message can be sent upstream by the attacked network node. For example, the message payload can contain a return address R, a network/host address H and/or a cookie generated by the attacked network node.

In some embodiments, an upstream router can look up H to check for a match in one or more lists of the local cache. If a match results, the router can forward a message upstream to appropriate interfaces. This can repeat recursively with routers further upstream.

In some embodiments, if an upstream router does not find H in the local cache, a report message can be sent to R with, for example, interface information of a downstream neighbor and the cookie. In some embodiments, this can be identified as an entry point of the attack, such as the flood.

Ricciulli, col. 3, ll. 16-43 (emphasis supplied).

This portion of *Ricciulli* manifestly does not teach the step of determining a logical entry point of an attack using a correlation engine to correlate the intrusion information and the network information. Instead, this portion of *Ricciulli* indicates that a data packet can be sent from the target of the attack upstream by the attacked network node. The data packet includes a network host address generated by the attacked network node. If an upstream router does not find the host address in the local cache, then a report is sent back to the target of the attack. Thus, the router that did not have a host address in its cache is identified as the source of the attack.

Ricciulli does not provide any teaching regarding logical entry points of attack, as claimed. *Ricciulli* does not provide any teaching regarding using a correlation engine to correlate intrusion

information and network information to determine a logical entry point of an attack, as claimed. Instead, *Ricciulli* teaches finding a physical entry point of the attack – the router lacking a host address in a cache – by sending a data packet from the target to that router. Nowhere does *Ricciulli* teach that a logical point is determined using a correlation engine as claimed in claim 5. *Ricciulli* does not even discuss logical entry points.

The examiner appears to assert that *Ricciulli* does teach something regarding logical entry points. However, the examiner's assertions regarding IP addresses being logical "representations" is wholly irrelevant to the claimed invention as recited in claim 5. If the examiner asserts that a TCP/UDP port is a logical entry point, the examiner is manifestly incorrect. In either case, the examiner's characterization of *Ricciulli* is manifestly incorrect.

Specifically, the examiner states that "IP addresses, as well as TCP/UDP ports are logical representations used in combination to identify the entry point." As a first matter, the examiner has mischaracterized the claim language. The claim language requires "determining a *logical entry point* of the attack using a *correlation engine* to correlate the *intrusion information and the network information*." The examiner does not indicate what IP addresses and TCP/UDP addresses logically represent. Nevertheless, whether or not IP addresses and TCP/UDP ports are logical representations of something is irrelevant. What is relevant is determining a *logical entry point* of an attack. Nowhere does *Ricciulli* teach determining a *logical entry point* of an attack. As shown above, *Ricciulli* teaches finding a *physical router* that is the source of an attack – not a logical entry point.

Additionally, the examiner's characterization of *Ricciulli* is manifestly incorrect. As shown above in the quoted text, *Ricciulli* teaches finding the *router* from whence an attack is originating. *Ricciulli* is unconcerned with determining a logical entry point of the attack, whether or not either the router that is the source of the attack or the server under attack is logically divided. *Ricciulli* only finds the *physical router* that is the source of the attack, not a logical entry point.

Nevertheless, the examiner asserts that the following text, in combination with the previously cited text, teaches the determining step as claimed:

FIG. 3 shows a flowchart 300 of an aspect of some embodiments for maintaining one or more lists of one or more network characteristics. Various embodiments can alter, add to, delete from, and/or reorder elements of the flowchart 300. In 310, messages can be prevented from transiting the first network node. One embodiment prevents by filtering. Some embodiments prevent, responsive to receiving a message from an attacked network node. The attacked network node may have received a flooding attack and/or a denial of service attack. Such messages can have suspicious instances of network characteristics of lists. The suspicious instances can be associated with attacks on attacked network nodes. In 315, *suspicious instances can be compared with repeatedly updated lists*. If the compare fails to result in a match, prevention can be halted. One embodiment of halting the preventing can include removing the filter. In 320, lists can be

repeatedly updated. Instances having low frequency of occurrences can be removed from lists. In various embodiments, the updating can occur at the second network node 140 and/or a third network node.

There are many possible network characteristics that can be matched in 3150. For example, IP source addresses 330, destination IP addresses 335, source TCP ports 340, source UDP ports 345, destination TCP ports 350, destination UDP ports 355, TCP flags 360, and/or ICMP flags 365.

Ricciulli, col. 4, l. 45 through col. 5, l. 2 (emphasis supplied).

This portion of *Ricciulli* does not teach the step of determining a logical entry point, either alone or together with the previously cited text. This portion of *Ricciulli* teaches comparing suspicious data packets with repeated updated lists. If some aspect of the data packet matches one or more aspects contained in the list, then a suspicious data packet is confirmed to be a data packet associated with an attack. In this case, the source or host of the attack is prevented from sending further data packets to the server. If a suspicious data packet is not associated with an attack, then communication from the source or host is allowed.

However, *Ricciulli* never teaches determining a logical entry point of an attack using a correlation engine, as claimed in claim 5. Although information in data packets is compared to information contained in lists, no comparison is made to determine a *logical entry point* of the attack. Instead, the comparison is made to determine whether a host or source should be blocked from sending further data packets. As described above, the host or source is detected by sending a search data packet upstream in the network to determine which router does not have a host address in a cache. That *physical* router is the source of the attack. Thus, *Ricciulli* does not teach the determining a logical entry point step, as claimed.

Additionally, *Ricciulli* does not teach "identifying a physical entry point associated with the logical entry point," as claimed in claim 5. The examiner asserts otherwise, citing the following portion of *Ricciulli* for support:

In some embodiments, an upstream router can look up H to check for a match in one or more lists of the local cache. If a match results, the router can forward a message upstream to appropriate interfaces. This can repeat recursively with routers further upstream.

In some embodiments, if an upstream router does not find H in the local cache, a report message can be sent to R with, for example, interface information of a downstream neighbor and the cookie. In some embodiments, this can be identified as an entry point of the attack, such as the flood.

Ricciulli, col. 3, ll. 34-43.

Again, the above-cited text teaches identifying a *physical* router as the source of attack. *Ricciulli* does not mention logical entry points and does not actually teach identifying a physical entry point associated with the logical entry point.

Nevertheless, the examiner also states that, "the physical entry point is where the router or node actually connects to the network, on its network interface." The examiner's statement is irrelevant, whether or not the statement is correct. As *Ricciulli* points out, a *physical* router is identified as the source of an attack. At no point does *Ricciulli* identify a *logical* entry point associated with the *physical* entry point. The disclosure simply does not exist in *Ricciulli*.

As shown above, *Ricciulli* does not teach either the "determining" step or the "identifying" step as claimed in claim 5. Accordingly, *Ricciulli* does not anticipate claim 5.

Claims 21 and 25 contain features similar to those presented in claim 5. Therefore, *Ricciulli* does not anticipate claims 21 and 25 for the reasons presented above. Because claims 6-15, 18-20, 22-24, 26, and 27 depend from claims 5, 21, or 25, the same distinctions between *Ricciulli* and the claimed invention in claim 5 can be made for these claims. Additionally, claims 6-15, 18-20, 22-24, 26, and 27 claim other additional combinations of features not suggested by the reference. For example, *Ricciulli* does not teach the claimed feature of alerting a network manager to the location of the logical port and of the physical port, as claimed in claim 22. Consequently, it is respectfully urged that the rejection of claims 6-15 and 18-27 have been overcome.

Furthermore, *Ricciulli* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Ricciulli* actually teaches away from the presently claimed invention because it teaches directly detecting a physical point of a network attack as opposed to detecting a physical point of an attack from a logical point of attack, as in the claimed invention. Absent the examiner pointing out some teaching or incentive to implement *Ricciulli* and the claimed features, one of ordinary skill in the art would not be led to modify *Ricciulli* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Ricciulli* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

II. 35 U.S.C. § 103, Asserted Obviousness

The examiner rejected claims 16 and 17 under 35 U.S.C. § 103 as obvious over *Ricciulli* in view of either *Skirmont*, et al. Method and Apparatus for Load Apportionment Among Physical Interfaces in Data Routers, U.S. Patent 6,553,005 (April 22, 2003) or over *Ricciulli* in view of *Hunt*, et al. Network Dispatcher: A Connection Router for Scalable Internet Services, IBM Almaden Research Center, San

Jose, CA, available at unizh.ch/home/mazzo/reports/www7conf/fullpapers/1899/com1899.htm. These rejections are respectfully traversed.

Both of these rejections rely on the flawed assertion that *Ricciulli* teaches all of the features of the underlying independent claims. As shown above, *Ricciulli* does not teach the claimed features of determining, as claimed, or identifying, as claimed.

Furthermore, nothing in *Ricciulli* suggests these claimed features. *Ricciulli* is devoid of disclosure regarding identifying logical points of entry for an attack and *Ricciulli* is devoid of disclosure regarding identifying a physical entry point associated with the logical entry point. Additionally, *Ricciulli* would not benefit from adding these features because *Ricciulli* already claims to be able to identify the physical source of the attack in the manner described above. Thus, no one of ordinary skill would have any reason to modify *Ricciulli* to achieve the claimed inventions.

Additionally, nothing in *Skirmont* or *Hunt* teaches or suggests the features of determining and identifying as claimed. Additionally, no teaching, suggestion, or motivation exists to modify *Ricciulli* to achieve the inventions of claims 16 and 17 in view of any reference. Accordingly, the examiner has failed to state *prima facie* obviousness rejections of claims 16 and 17. For similar reasons, claims 16 and 17 are non-obvious over the cited references. Accordingly, the rejection under 35 U.S.C. § 103 has been overcome.

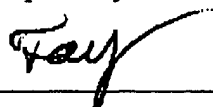
III. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: April 11, 2006

Respectfully submitted,



Theodore D. Fay III
Reg. No 48,504
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants